CLAIMS

1. A method of encrypting information transmitted between a fixed network (MSC, BSS) and a mobile station (MS) in a mobile radio system that operates in accordance with the time division multiple access concept, wherein the information is divided into at least two blocks (B1, B2) and transmitted in at least two time slots (TS1, TS2) corresponding to said blocks in each frame in a frame sequence, and wherein encryption is effected by

a) forming a pseudo-random sequence (PS) in accordance with a given encryption algorithm (A5) from an encryption key (Kc) and the ordinal number (FN) of the frame in which the information is transmitted;

b) performing a logic operation (EXOR) between said pseudo-random sequence (PS) and each block (B1 and B2) of the non-encrypted information to obtain encrypted information (BK1, BK2);

characterized by

c) modifying said encryption key (Kc) in accordance with a given algorithm (ALG1) and in dependence on the ordinal number of a time slot (TSn) so as to obtain a modified encryption key (Kc');

d) forming a modified pseudo-random sequence (PSm') from the resultant modified encryption key (Kc') in accordance with aid encryption algorithm A5); and

e) performing said logic operation (EXOR) on the modified pseudo-random sequence (PSm') and for each block (B1 and B2) of the non-encrypted information.

2. A method according to Claim 1, **characterized** by carrying out the operation performed in accordance with e) on the information block (B1) that belongs to the time slot (TS1) whose ordinal number has been used to form said modified encryption key.

3. A method of encrypting information transmitted between a fixed network (N) and a mobile station (MS) in a mobile radio system that operates in accordance with the time division multiple access concept, wherein the information is divided into at least two blocks (B1, B2) and transmitted in at least two time slots (TS1, TS2) corresponding to said blocks in each frame in a frame sequence, and wherein encryption is effected by

a) forming a pseudo-random sequence (PS) in accordance with a given encryption algorithm (A5) from an encryption key (Kc) and the ordinal number (FN) of the frame in which the information is transmitted;

b) performing a logic operation (EXOR) between said pseudo-random sequence (PS) and each block (B1 and B2) of non-encrypted information to obtain encrypted information (BK1, BK2);

characterized by

c) modifying said frame number (FN) in accordance with a given algorithm (ALG2) and in dependence on the ordinal number of a relevant time slot (TSn);

d) forming a modified pseudo-random sequence (PSm') from the obtained modified frame number (FN') in accordance with said encryption algorithm (A5); and

e) performing said logic operation (EXOR) on the modified pseudo-random sequence (PSm') for each block (B1 and B2) of non-encrypted information.

4. A method of encrypting information transmitted between a fixed network (N) and a mobile station (MS) in a mobile radio system that operates in accordance with the time division multiple access concept, wherein the information is divided into at least two blocks (B1, B2) and transmitted in at least two time slots (TS1, TS2) corresponding to said blocks in each frame in a frame sequence, and wherein encryption is effected by

a) forming a pseudo-random sequence (PS) from an encryption key (Kc) and the ordinal number (FN) of the frame in which

the information is transmitted in accordance with a given encryption algorithm (A5);

b) performing a logic operation (EXOR) between said pseudo-random sequence and each block of the non-encrypted information (INFO1);

characterized by

c) modifying said encryption key (Kc) in accordance with a given algorithm (ALG1) and in dependence on the ordinal number of the relevant time slot (TSn);

d) forming a modified pseudo-random sequence (PSm') from the obtained modified encryption key (Kc') in accordance with said encryption algorithm (A5);

e) modifying said frame number (FN) in accordance with a given algorithm (ALG2) and in dependence on the ordinal number of a relevant time slot (TSn);

f) forming a modified pseudo-random sequence (PSm') from the obtained modified frame number (FN') in accordance with said encryption algorithm (A5); and

g) performing said logic operation (EXOR) on the modified pseudo-random sequence (PSm') for each block (B1 and B2) of the non-encrypted information.

Sub A2

5. A method of encrypting information transmitted between a fixed network (N) and a mobile station (MS) in a mobile radio system that operates in accordance with the time division multiple access concept, wherein the information is divided into at least two blocks (B1, B2) and transmitted in at least two time slots (TS1, TS2) corresponding to said blocks in each frame in a frame sequence, and wherein encryption is effected by

a) forming a pseudo-random sequence (PS) from an encryption key (Kc) and the ordinal number (FN) of the frame in which the information is transmitted in accordance with a given encryption algorithm (A5);

b) performing a logic operation (EXOR) between said pseudo-random sequence and each block of the non-encrypted information (INFO1);

characterized by

c) forming a modified pseudo-random sequence (PSm') from said pseudo-random sequence (PS) in dependence on the ordinal number (TSn) of the time slot within which the information block (B1 or B2) that is encrypted with the modified pseudo-random sequence shall be transmitted in accordance with a given algorithm (ALG3); and

d) performing said logic operation (EXOR) on the modified pseudo-random sequence (PSm') for each block (B1 and B2) of the non-encrypted information.